一种基于尺度不变局部特征的零低频信息隐藏算法 *

任　帅[1a]，贺　媛[1a]，柳雨农[1b]，徐振超[1a]，张　弢[1b†]，王　震[1a]，慕德俊[2]

(1. 长安大学 a. 信息工程学院; b. 电子与控制工程学院，西安 710064; 2. 西北工业大学 自动化学院，西安 710072)

摘　要：针对目前信息隐藏算法抵抗隐写分析能力弱的问题，提出一种基于尺度不变（binary robust invariant scalable keypoints，BRISK）局部特征的零低频信息隐藏算法。首先，对载体图像进行一阶 CL 多小波变换，在低频 LL2 中提取 BRISK 特征点生成图像特征矩阵；其次，利用 zig-zag 和 Logistic 混沌置乱对秘密信息做去相关性处理；再次，将图像特征与加密信息通过对比特征值形成关联序列；最后，将关联序列嵌入到高频 HL2、HH2 的低 3 位。算法将高能量区域的特征矩阵与两次加密信息所构建的关联信息隐藏于高频区域，有利于算法的鲁棒性和抗分析性。在高阶统计量对 200 幅图片的分析测试下，最大检出率低于 7.516%，表明所提算法具有良好的抗分析性。

关键词：零低频信息隐藏；BRISK 特征；CL 多小波变换；抗分析性

中图分类号：TP309.2　　doi: 10.3969/j.issn.1001-3695.2018.06.0318

Zero-low-frequency information hiding algorithm based on local BRISK feature

Ren Shuai[1a], He Yuan[1a], Liu Yunong[1b], Xu Zhenchao[1a], Zhang Tao[1b†], Wang Zhen[1a], Mu Dejun[2]

(1. *a. School of Information Engineering*, *b. School of Electronic & Control Engineering*, *Chang'an University*, *Xi'an* 710064, *China*; 2. *College of Automation*, *Northwestern Polytechnical University*, *Xi'an* 710072, *China*)

Abstract: Aiming at inferior anti-analysis of current information hiding algorithm, this paper proposed a zero-low-frequency information hiding algorithm based on local BRISK feature. . First, it carried out first-order CL multi-wavelet transform for carrier image. then extracted BRISK feature points in the low-frequency LL2 to generate an image feature matrix; Second, Using zig-zag scrambling and logistic chaos scrambling for the secret image to decorrelate; Again, associated the image feature with the encrypted information to form an association sequence by comparing feature values; Last, it would embed association sequence into lower three bits of high-frequency HL2 and HH2. The association information constructed by eigenmatrix of high energy region and encrypted information of two times was hidden in the high frequency region, which was beneficial to the robustness and anti-analysis of algorithm. Under the analysis of high-order statistics on 200 pictures, the maximum detection rate was less than 7.516%, which indicates that the proposed algorithm has good anti-analysis ability.

Key words: zero-low-frequency information hiding; BRISK feature; CL multi-wavelet transform; anti-analysis ability

0　引言

随着网络信息爆炸式的增长，信息安全备受关注。信息隐藏作为信息安全领域的一个重要分支，是实现秘密通信的重要手段，成为目前研究的热点。在近几年的数字图像信息隐藏算法中，文献[1]将载体 JPEG 彩色图像按 8×8 分块后转到 YCbCr 空间，对 3 个分量实施 4 级离散小波变换，组合每块低频系数用于隐藏信息，鲁棒性强，但 PSNR 较低，不可见性差；文献[2]利用整数小波变换和二进制比特分组，将灰度密图的十进制矩阵整除所得的商和余数分别嵌入低频和高频，专注于鲁棒性，但低频系数改动较大，影响图像视觉效果；文献[3]通过调整 W 变换频谱中两个随机系数的大小完成信息嵌入，由于一直修改的是同一系数对“[2,3]和[4,1]”，所以局部特征变换明显；文献[4]结合 CL 多小波变换与组合位平面理论，根据数字图像能量分布特性隐藏相应信息，但低频中隐藏鲁棒信息种类较多，不可见性相对较差；文献[5]通过结合压缩感知和 GHM 多小波变换，替换对应奇异值实现信息隐藏，奇异值虽具有稳定性，但大面积修改奇异值使传输图像特征变化明显，容易引起外界攻

收稿日期：2018-06-14；**修回日期：**2018-07-22　**基金项目：**国家自然科学基金资助项目（61702050，61402052）；国家级大学生创新创业训练计划资助项目（201610710036）

作者简介：任帅（1982-），男，山西太原人，副教授，博士，主要研究方向为信息隐藏理论与模型；贺媛（1994-），女，陕西神木人，硕士研究生，主要研究方向为 3D 模型处理与应用；柳雨农（1993-），男，甘肃平凉人，硕士研究生，主要研究方向为非常规载体信息隐藏；徐振超（1992-），男，山西长治人，硕士研究生，主要研究方向为信息隐藏、数字信息技术；张弢（1984-），女（通信作者），山西吕梁人，副教授，博士，主要研究方向为多载体信息隐藏技术（zt904@foxmail.com）；王震（1993-），男，山西运城人，硕士研究生，主要研究方向为多媒体数据检索及认证；慕德俊（1963-），男，山东荣成人，教授，博导，主要研究方向为网络与信息安全。

击；文献[6]通过修改载体图像在 AMBTC 域生成的高低均值序列的直方图特征完成信息嵌入，直方图变化会引起图像失真问题。综上所述，以上信息隐藏算法都是通过修改数字图像特征改变相对重要位置像素直接隐藏，不可见性差。攻击者可以根据变换的图像特征进行隐写分析，抗分析性能弱是以上算法存在的共有问题。

零数字水印技术是通过建立载体图像的某个特征与数字水印的映射关系实现嵌入，整个过程不会修改图像特征，因此不会引起人们注意，具有抵抗隐写分析的特性。考虑到低频包含一幅数字图像的主要信息，本文算法将零的思想与低频结合，提出以零低频技术为基础的信息隐藏思路。在获取数字图像低频时考虑到主要信息量要足够大以致于可近似于原图像，选取 CL 多小波变换。在建立特征映射关系时考虑到鲁棒性，尤其是抗剪切性的要求，选择在计算机视觉领域广泛应用的 BRISK 特征。在秘密信息嵌入和提取的安全性方面，考虑到去相关性能提升安全性，选取了具有扰乱位置性能的 zig-zag 及伪随机性良好能改变像素值的 Logisti 混沌序列，最终实现了一种基于 BRISK 特征的零低频信息隐藏算法。该算法先在 CL 多小波变换后的低频中提取 BRISK 特征点生成图像特征矩阵；再利用 zig-zag 和 Logistic 混沌置乱对秘密信息做去相关性处理；然后生成图像特征与加密信息的关联序列；最终将关联序列嵌入到高频。在 MATLAB 环境中实验测试表明，本文提出算法具有很好的不可见性、鲁棒性、感知篡改性和抗隐写分析能力。

1　本文信息隐藏算法

本文提出的信息隐藏算法主要分为四个阶段：a)对载体图像进行一阶 CL 多小波变换；b)依据 CL 多小波变换后独特的高低能量对立分布的特性，在高能量 LL_2 区域寻找 BRISK 特征点，根据分布状况提取纹理复杂度高区域的特征点；c)将提取的特征点按照 BRISK 特征提取算法生成 512 位二进制序列的特征描述子，每 8 位组合转换为十进制，生成 8×8 大小的图像特征矩阵；d)将隐藏信息与特征矩阵建立关联实现信息隐藏。

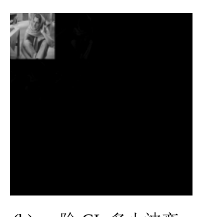
1.1　CL 多小波变换处理

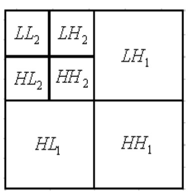
CL 多小波变换是利用对称性构造的一种多小波，具有短支撑性、二阶消失矩和正交性等显著特点，且 CL 多小波变换后能量集中于最低分辨率子图的低频 LL_2 区域[7]，具体能量分布如表 1 所示。利用上述特性，本文对载体图像进行一阶 CL 多小波变换（图 1），在占有原图 96.53%的能量低频 LL_2 区域提取特征向量，保证算法鲁棒性和抗分析性。将秘密信息生成的关联信息嵌入到占有原图 97.36%的能量低频 LL_1 分解后的高频 HL_2 和 HH_2 区域，保证算法的鲁棒性和不可见性。

表 1　CL 多小波变换的一阶能量分布

CL 多小波变换 LL_1 子图像能量占图像总能量的百分比/%	LL_1 子图像各个分量的能量分/%			
	LL_2	LH_2	HL_2	HH_2
97.36	96.53	2.51	0.62	0.34


(a) 原始图像


(b) 一阶 CL 多小波变换



(c) 子分量分布示图

图 1　对载体图像进行一阶 CL 多小波变换

1.2　提取 BRISK 特征点

BRISK 特征点是一种具有旋转不变性、尺度不变性及抗噪抗压缩等鲁棒性好的特征点[8]。在金字塔尺度空间上利用 FAST9-16 算子检测特征点，对于满足 FAST 标准的点进行非极大值抑制，对极大值点进行亚像素插值来精确定位（图 2），得到特征点的位置和尺度 t。

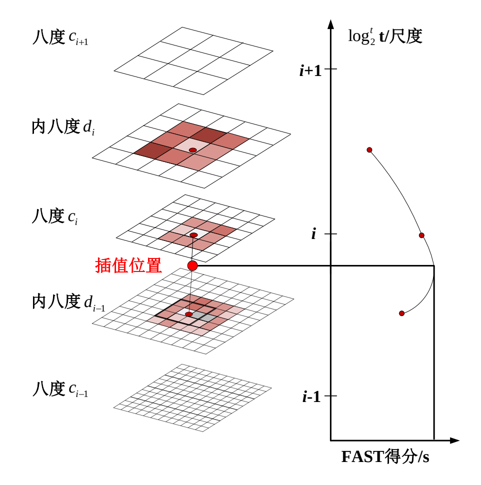


图 2　亚像素插值精确定位

图 2 中金字塔尺度空间是由 4 个八度和 4 个内八度构造而成，其中八度用 c_i 表示，内八度用 d_i 表示，i=0，1，2，3。c_0 表示原图像，d_0 是原图像的 1.5 倍下采样，相邻八度和相邻内八度都是 2 倍下采样的关系。且八度及内八度与原图像的尺度关系为 $t(c_i)=2^i$，$t(d_i)=2^i$。

本文在一阶 CL 多小波变换后的低频分量 LL_2 中提取特征点。由于 BRISK 特征点对应图像中像素突变点，邻域内特征点数目越多，纹理越强，即为一幅图像的重要区域。以此为衡量标准，选择复杂纹理区域的鲁棒特征点，具有不易丢失的特性，原因在于该区域如果遭受剪切攻击，图像就会失去传输意义。为此，若某特征点邻域内特征点数目最多，则选择该特征点生成特征描述子。特征点邻域半径根据式（1）自适应确定。

$$R = \kappa t \quad (1)$$

其中：κ 为常量，以控制邻域半径的大小；t 为特征点尺度值，具有缩放不变性。

1.3　生成图像特征矩阵

以 1.2 节选择出的特征点为中心，定义 4 个不同半径离散同心圆的采样模式，如图 3 所示。

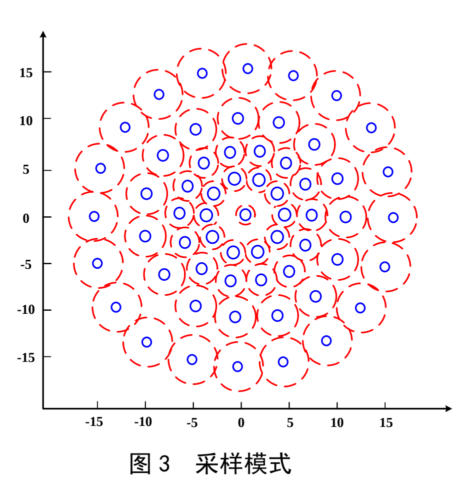


图 3 采样模式

在圆上等间隔获取 60 个采样点，对采样点先进行高斯滤波消除邻域采样模式的混叠效应后两两组对，总计 60*(60-1)/2 对。设置阈值，将采样点对分为短距离点对和长距离点对。本文实验时采用 Stefan 原算法 BRISK 中所用的阈值，即短距离点对阈值为 9.57t，长距离点对阈值为 13.67t。将特征点采样模式按照式（2）旋转，保证旋转不变性。

$$\alpha = \arctan 2(g_x, g_y) \tag{2}$$

其中：(g_x, g_y) 为特征点主方向。特征点主方向由长距离点对的局部梯度确定，如式（3）所示。

$$g = \begin{pmatrix} g_x \\ g_y \end{pmatrix} = \frac{1}{l} \times \sum_{(p_i, p_j)\in L} g(p_i, p_j) \tag{3}$$

其中：l 为长距离点对数；L 为长距离点对集合；$g(p_i, p_j)$ 为 (p_i, p_j) 采样点对的局部梯度。选择 512 个短距离点对按照式（4）方式进行强度值比较，比较结果为二进制编码，得到 512 位二进制序列特征描述符。

$$b = \begin{cases} 1, I(p_j^\alpha, \sigma_j) > I(p_i^\alpha, \sigma_i) \\ 0, others \end{cases} \tag{4}$$

其中：$\forall (p_i^\alpha, p_j^\alpha) \in S$，$I(p_i^\alpha, \sigma_i)$，$I(p_j^\alpha, \sigma_j)$ 为旋转 α 角度后 p_i、p_j 点像素值；σ_i、σ_j 为 p_i、p_j 点尺度。

本文将计算得到的特征点描述子，即 512 位二进制序列记为 $\boldsymbol{L}$。将 $\boldsymbol{L}$ 从左到右按 8 位转换为十进制整型数，则 512 位二进制序列描述子共转换为 64 个 0~255 的整型数。逆序排列得到 8×8 方阵作为图像特征矩阵，记为 $\boldsymbol{J}$ 矩阵。

1.4 隐藏信息嵌入步骤

a)对秘密图像 $\boldsymbol{T}$ 进行 zig-zag 置乱处理[9]，置乱遵循本文设计的规则：从矩阵右下角开始按“之”字形自下向上扫描，将扫描像素值存入一维数组 $\boldsymbol{S}$。逆序排列 $\boldsymbol{S}$ 生成一维数组 $\boldsymbol{S}_0$，满足 $\boldsymbol{T} = \boldsymbol{S}_0$。迭代次数 Z=10，得到置乱图像 $\boldsymbol{W}$。

b)对 $\boldsymbol{W}$ 执行 Logistic 混沌映射置乱[10]，见式（5），确定 Logistic 控制参数 μ 和初始值 t_0，得到混沌序列 $\boldsymbol{T_m}$。置乱规则：将 $\boldsymbol{W}$ 平均分成 16 块，依次在每块中顺序取一个像素点放入 G 中。其次，将 $\boldsymbol{T_m}$ 的前 8 位作为置换向量 $\boldsymbol{A}$，后 8 位作为置换向量 $\boldsymbol{B}$。按照表 2 规则，根据 $\boldsymbol{T_m}$ 每相邻两位的取值确定 G 中对应值与 $\boldsymbol{A}$ 或者 $\boldsymbol{B}$ 按位“异或”或“同或”得到新灰度值。置乱后的比特序列记为 $\boldsymbol{D}$。

$$t_{n+1} = \mu t_n (1 - t_n) \tag{5}$$

表 2 Logistic 置乱规则

$\boldsymbol{T_m}$ 相邻两位	$\boldsymbol{A}$	$\boldsymbol{B}$
00		异或
01		同或
10	异或	
11	同或	

c)任取 4 个 0-7 的整型随机数 e、f、g、h，构造 (e,f)，(g,h) 作为 $\boldsymbol{J}$ 矩阵的两个坐标点，比较 $J(e,f)$ 与 $J(g,h)$ 的大小。若 $J(e,f) = J(g,h)$，则需重新选取 4 个值（可重复选取），否则按表 3 方式将 $\boldsymbol{J}$ 矩阵与秘密序列 $\boldsymbol{D}$ 按位建立关联信息。重复步骤 c)，直至将秘密序列 $\boldsymbol{D}$ 所有位与 $\boldsymbol{J}$ 矩阵建立关联，然后将关联信息串行连接形成关联序列 $\boldsymbol{K}$。

表 3 秘密序列 $\boldsymbol{D}$ 与特征矩阵 $\boldsymbol{J}$ 建立关联

条件	$\boldsymbol{D}$	关联信息
$J(e,f) > J(g,h)$	0	$ghef$
	1	$efgh$
$J(e,f) < J(g,h)$	0	$efgh$
	1	$ghef$

d)将关联序列 $\boldsymbol{K}$ 按行排列顺序分别隐藏到分量 HL_2、HH_2 系数的低 3 位中，记为 $\boldsymbol{C}_{HL_2}^0$、$\boldsymbol{C}_{HL_2}^1$、$\boldsymbol{C}_{HL_2}^2$、$\boldsymbol{C}_{HH_2}^0$、$\boldsymbol{C}_{HH_2}^1$、$\boldsymbol{C}_{HH_2}^2$。隐藏规则：若关联序列第 n(n=0，1，2，3....)位是 3，转换为二进制是 011；若 HL_2 或 HH_2 第 n 个系数低 3 位是 010，则修改最后一位 0 为 1，即完成 3 的嵌入。低 3 位可能有 8 种情况，分别是 000、001、010、011、100、101、110、111。无论要隐藏的是关联序列中 0~7 的哪一个数值，嵌入修改位数的概率都是：修改一位或两位为 3/8，修改三位或不修改为 1/8。低修改率保证嵌入信息的不可见性。

e)将 zig-zag 置乱参数 Z 和 Logistic 置乱参数 μ、t_0 依次嵌入到 LH_2 分量。

f)对图像进行一阶 CL 多小波逆变换得含密图像 $\boldsymbol{T_{sre}}$。

1.5 信息提取步骤

本文算法为基于 BRISK 特征的零低频算法，与信息嵌入过程类似。

a)对含密图像 $\boldsymbol{T_{sre}}$ 进行一阶 CL 多小波变换，分解出子分量图 LL_2、LH_2、HL_2、HH_2。

b)在 LL_2 区域提取出 BRISK 特征点，根据保存的特征点描述子 $\boldsymbol{L}$，寻找与之匹配的特征点 C，然后按照本文 1.3 节中步骤生成图像特征矩阵 $\boldsymbol{J}'$。

c)依次取出 HL_2 分量系数的低 3 位转换为一个十进制数，串行连接得到关联序列 $\boldsymbol{K}'$。依次读取 4 个数 e、f、g、h，顺序组成坐标点 (e,f)，(g,h)。在矩阵 $\boldsymbol{J}'$ 中比较两个位置对应数值的大小，若 $J'(e,f) < J'(g,h)$，则表示存入信息为“0”；若 $J'(e,f) > J'(g,h)$，则表示存入信息为“1”，依次解码得到秘密序列 $\boldsymbol{D}'$。同理，对 HH_2 分量也进行上述操作，得到秘密序列 $\boldsymbol{D}''$。

d)确定秘密序列。接收者通过比较 $\boldsymbol{D}'$ 与 $\boldsymbol{D}''$ 判断信息传输

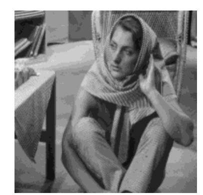
过程是否受到外界攻击，若两者一致，说明信息安全传输；若两者不一致，查看两序列长度，完整则说明没有受到攻击，明显短缺则说明受到攻击。此时，选择 $\boldsymbol{D}'$ 或 $\boldsymbol{D}''$ 中的完整序列作为最终提取的秘密序列。

e)在 LH_2 区域提取出两次置乱所有参数 Z、μ、t_0。利用 Logistic 置乱参数 μ、t_0 对秘密序列 $\boldsymbol{D}'$ 或 $\boldsymbol{D}''$ 进行逆置乱变换，得到置乱后序列 $\boldsymbol{W}'$。利用 zig-zag 置乱参数 Z 对 $\boldsymbol{W}'$ 进行逆置乱，得到原始秘密信息 $\boldsymbol{T}'$。

2　实验与结果分析

对本文算法进行实验仿真，实验环境是 MATLAB R2013a，所选载体图像为 512×512 的“barbara”灰度图，如图 4（a）所示；秘密图像为 64×64 的“baboon”二值图，如图 4（b）所示；实验仿真后得到的含密图像如图 4（c）所示。





(a) 载体图像　　(b) 秘密图像　　(c) 含密图像

图 4　嵌入信息前后的可视图像示意

2.1　不可见性实验

取 100 幅（512×512）图像用本文隐藏算法测试，结果如图 5 所示。图中横坐标表示嵌入量 2^k，纵坐标是峰值信噪比（peak signal-to-noise ratio，PSNR）[11]。数据显示，当 k=14 时，嵌入量为 16384 bits，$PSNR$=42.082，故得 k≤14 算法具有较高不可见性。

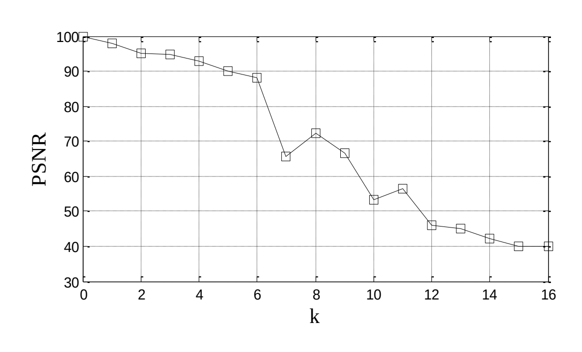


图 5　不可见性实验结果

依据 PSNR，在相同嵌入强度下，将本文混合域算法（记为 BRISK-ZLF）与频域算法修改 W 变换系数对的文献[3]（记为 W-W）和混合域算法修改 AMBTC 域直方图特征的文献[6]（记为 AMBTC-HS）进行不可见性对比，比较结果如表 4 所示。BRISK-ZLF 的 PSNR 平均值为 42.625，W-W 的 PSNR 平均值为 38.204，BRISK-ZLF 相比 W-W 不可见性提高 11.57%。AMBTC-HS 的 PSNR 平均值为 41.235，与本文 BRISK-ZLF 接近，在嵌入强度为 0.125 和 0.25 时，AMBTC-HS 的 PSNR 值保持相对稳定且稍大于 BRISK-ZLF。由于此时的嵌入区域遇到高低均值序列相等的块，移位后没有影响。且从理论角度出发，当嵌入强度大于 0.25 时，AMBTC-HS 实施嵌入时还是会偶尔遇到高低均值序列相等块，也有可能根据载体图像像素分布的不同，使得某些载体图像会频繁遇到高低均值序列相等块，从而具有高 PSNR 值。而且 AMBTC-HS 算法采用 512×512 图像的 AMBTC 域作为嵌入域，而本文算法仅仅选择了大小为 128×128 的两个高频区域，显然 AMBTC-HS 的可嵌入强度要高于本文算法。也就是说，本文算法的容量性相对较低。但在本文所做实验嵌入强度小于等于 0.25 的情况下，求取整体的平均值，本文 BRISK-ZLF 的不可见性性能要好于 AMBTC-HS。

表 4　不可见性实验对比

嵌入强度	PSNR/dB		
	BRISK-ZLF	W-W	AMBTC-HS
0.015625	46.083	41.178	42.193
0.031250	44.976	40.231	41.174
0.062500	42.082	38.418	41.053
0.125000	40.000	37.079	40.906
0.250000	39.983	34.116	40.848
平 均 值	42.625	38.204	41.235

2.2　鲁棒性实验

鲁棒性是检验算法的健壮性，即反映秘密信息经攻击处理后的完整性程度。本文算法在秘密信息提取时需要重新提取出 BRISK 特征点，所以对算法鲁棒性检验至关重要。归一化相关系数（normalized cofficient，NC）用于衡量两幅图像的相似度，因此本文采用 NC 值作为鲁棒性批判标准。NC 值越大，表明秘密信息完整度越高，鲁棒性越好。NC 定义如式（6）所示。

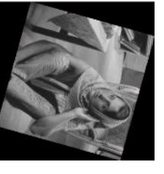
$$NC=\frac{\sum_{i,j}w(i,j)\hat{w}(i,j)}{\sqrt{\sum_{i,j}w(i,j)^2}\sqrt{\sum_{i,j}\hat{w}(i,j)^2}} \tag{6}$$

其中：$w(i,j)$、$\hat{w}(i,j)$ 分别是秘密信息和提取出的秘密信息在对应 i,j 坐标点的像素值。

本实验设计对含密图像进行剪切、旋转、缩放、椒盐噪声和高斯噪声以及滤波攻击处理，从受攻击的含密载体图像中提取秘密信息，实验结果如图 6 所示。




(a) cutting_18%　NC=0.974




(b) rotating=100.5°
NC=0.56

(c) shrinking_30%　NC=0.903



(d) enlengement_100%
NC=1




(e)'salt & peper'_d=0.16
NC=0.611




(f)Gaussi_μ=0.1，σ^2=0.004
NC=0.79




(g) winner2 filter_[3,3]
NC=0.854

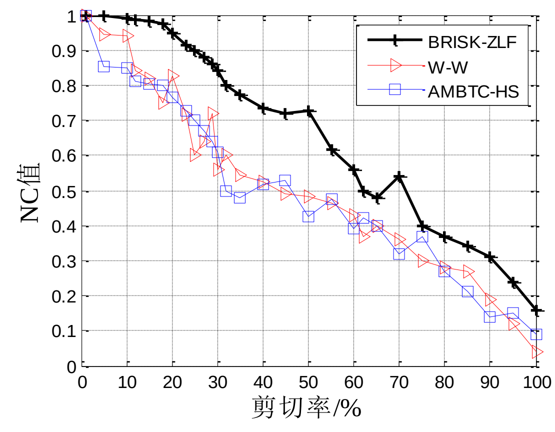



(h)medfilter_[5,5]
NC=0.69

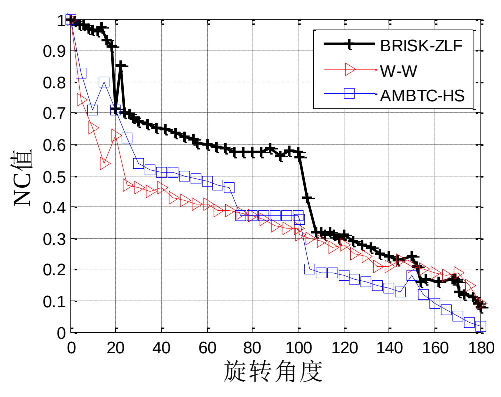
图 6　攻击及还原信息鲁棒性实验结果

根据图 6 可视化实验结果可得，当归一化相关系数 NC 达到 0.56 时，提取出的秘密信息便可辨识。用 NC 同时判断剪切与旋转攻击的鲁棒性如图 7 中的“BRISK-ZLF”实验数据所示，当剪切率小于 60%，旋转角度小于 100.5 时，NC≥0.56，表明本文算法具有很强的鲁棒性。

依据 NC 值，将 BRISK-ZLF 与 W-W 和 AMBTC-HS 进行鲁棒性对比，剪切攻击与旋转攻击的实验对比结果如图 7 所示。



（a）　剪切攻击对比实验



(b)　旋转攻击对比实验

图 7　剪切和旋转攻击对比实验

由图 7（a）可知，当剪切率为 45%时，BRISK-ZLF 提取秘密信息的 NC 值为 0.719，W-W 和 AMBTC-HS 的 NC 值分别是 0.490 和 0.530，比较即 BRISK-ZLF 的 NC 值分别提高 46.73%和 35.66%。由图 7（b）可知，当旋转 60°时，BRISK-ZLF 的 NC 值为 0.598，W-W 和 AMBTC-HS 的 NC 值分别是 0.410 和 0.480，即 BRISK-ZLF 的 NC 值分别提高 45.85%和 24.58%。综合剪切和旋转攻击实验数据，本文 BRISK-ZLF 算法的 NC 平均值为 0.601，W-W 的 NC 平均值为 0.452，AMBTC-HS 的 NC 平均值为 0.483。因此，本文算法鲁棒性分别提高 32.96%和 24.43%。

2.3　感知窜改性实验

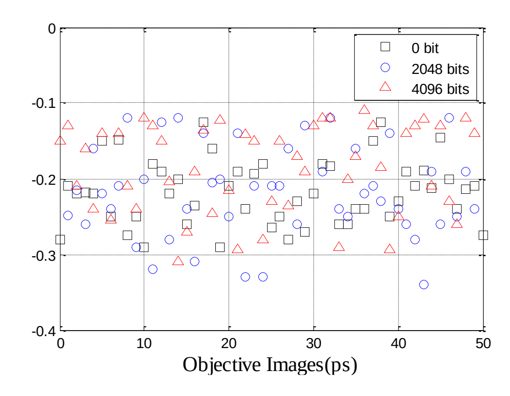
对从 HL_2 和 HH_2 中提取到的 $\boldsymbol{D'}$ 与 $\boldsymbol{D''}$ 进行对比校验，当剪切率为 6%，旋转 10°，缩放 5%，椒盐噪声（d=0.05），白噪参数（0.1，0.004），维纳滤波（[3，3]）的检出率如表 5 所示，计算得平均检出率为 96.22%，表明本文算法具有很高的感知篡改能力。

表 5　攻击对应感知篡改性检出率(200 张图片)

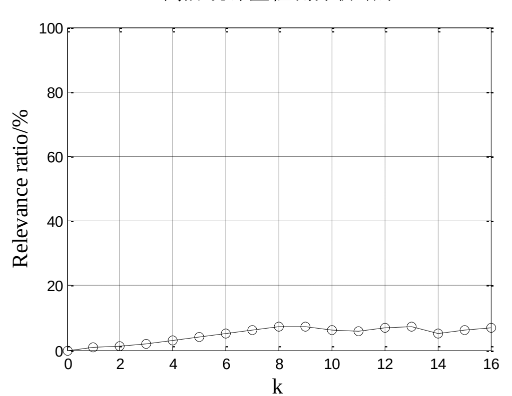
图像处理	剪切	旋转	缩放	椒盐噪声	白噪参数	滤波
检出率/%	99.56	97.26	99.37	96.21	89.22	95.71

2.4　抗分析性实验

抗分析性实验是本文的重点实验。在信息隐藏中，抗分析性是对一种算法性能的宏观把控。必须在保证不可见性、鲁棒性，一定容量性的前提下，才有可能具有强的抗隐写分析能力。本文将两次置乱完全去除相关性的秘密信息与图像低频 BRISK 特征建立关联序列，关联序列的最终隐藏区域为一阶 CL 多小波变换的高频 HL_2、HH_2 的低 3 位，隐藏区域隐蔽性强。现利用基于小波系数的高阶统计量分析算法对本文算法进行检测分析[12]，实验结果如图 8（a）所示。



（a）高阶统计量检测分析结果



（b）高阶统计量检测分析法的检出率

图 8　本文算法高阶统计量检测分析结果

分析图 8（a）实验数据，在 50 幅随机图片中，无法找出分离隐藏信息前后的一个甚至多个阈值。使用 200 幅图片进行检验测试，得图 8（b）测试结果，最大检出率低于 7.156%，表明本文算法具有强抗分析性。

3 结束语

本文提出一种基于 BRISK 特征的零低频信息隐藏算法。BRISK 特征本身具有鲁棒性，再加之低频提取，算法鲁棒性可进一步增强。零低频即是只在低频提取特征，最终嵌入区域还是高频，增强算法抗分析性。在隐藏区域的设计方面，本文算法利用能量可以忽略不计的高频隐蔽性强的低 3 位进行信息隐藏，且修改位数小于等于 3。秘密信息双置乱去除相关性，最终隐藏的信息实质是关联序列，算法的抗分析性在理论上有显著提高。此外，算法设计在高频 HL_2、HH_2 两块区域嵌入相同信息，获得高达 96.22%的检错感知性能。今后将考虑如何增大算法容量性，主要从隐藏区域的选取和秘密信息嵌入前的压缩预处理两方面进行研究，研究要遵循容量性和不可见性并存的原则。

参考文献：

[1] 刘艳波. 基于 JPEG 图像的改进小波变换信息隐藏算法 [J]. 北华大学学报：自然科学版, 2017, 18 (5): 697-700. (Liu Yanbo. Information hiding algorithm of wavelet transform based on JPEG image [J]. Journal of Beihua University: Natural Science, 2017, 18 (5): 697-700.)

[2] 蔡正保. 一种改进的基于小波变换的数字图像隐藏算法研究与实践 [J]. 佳木斯大学学报：自然科学版, 2015, 33 (6): 861-863. (Cai Zhengbao. Research and practice of an improved digital image hiding algorithm based on wavelet transform [J]. Journal of Jiamusi University: Natural Science Edition, 2015, 33 (6): 861-863.)

[3] 贺子恒, 张佳文, 侯桐, 等. 一种新的基于频域的图像信息隐藏方法 [J]. 软件导刊, 2014, 13 (5): 167-169. (He Ziheng, Zhang Jiawen, Hou Tong, *et al.* A new image information hiding method based on frequency domain [J]. Journal of Software, 2014, 13 (5): 167-169.)

[4] 张弢, 任帅, 巨永锋, 等. 基于 CL 多小波变换和组合位平面理论的秘密信息共享算法 [J]. 计算机应用, 2013, 33 (11): 3232-3234. (Zhang Tao, Ren Shuai, Ju Yongfeng, *et al.* Secret information sharing algorithm based on CL multi-wavelet transform and combination bit plane for confidential communication [J]. Journal of Computer Applications, 2013, 33 (11): 3232-3234.)

[5] 张弢, 康缘, 任帅, 等. 基于压缩感知和 GHM 多小波变换的信息隐藏算法 [J]. 计算机应用, 2017, 37 (9): 2581-2584. (Zhang Tao, Kang Yuan, Ren Shuai, *et al.* Information hiding algorithm based on compression sensing and GHM multi wavelet transform [J]. Journal of Computer Applications, 2017, 33 (11): 3232-3234.)

[6] 张弢, 柳雨农, 邢亚林, 等. 基于直方图移位的 AMBTC 域无损信息隐藏 [J/OL]. 计算机应用研究, 2019, 36 (6): 1-8 [2018-04-08]. http://kns. cnki. net/kcms/detail/51. 1196. TP. 20180408. 1051. 076. html. (Zhang Tao, Liu Yunong, Xing Yalin, *et al.* Lossless information hiding in AMBTC domain based on histogram shift [J/OL]. Application Research of Computers, 2019, 36 (6): 1-8 [2018-04-08]. http://kns. cnki. net/kcms/detail/51. 1196. TP. 20180408. 1051. 076. html.)

[7] 徐涛, 吴登峰, 刘杰, 等. 多小波正交扩充算法在图像处理中的应用 [J]. 吉林大学学报：工学版, 2006 (5): 778-781. (Xu Tao, Wu Dengfeng, Liu Jie, *et al.* Application of multiwavelet orthogonal expansion algorithm in image processing [J]. Journal of Jilin University: Engineering Science, 2006 (5): 778-781.)

[8] Leutenegger S, Chli M, Siegwart R Y. BRISK: binary robust invariant scalable keypoints [C]// Proc of International Conference on Computer Vision. 2011: 2548-2555.

[9] 陆萍, 董虎胜, 马小虎. 一种基于扩展 ZigZag 与位交换的图像置乱算法 [J]. 计算机应用与软件, 2012, 29 (10): 310-313. (Lu Ping, Dong Husheng, Ma Xiaohu. An image scrambling algorithm based on extended ZigZag and bit exchange [J]. Computer Applications and Software, 2012, 29 (10): 310-313.)

[10] 张永红, 张博. 基于 Logistic 混沌系统的图像加密算法研究 [J]. 计算机应用研究, 2015, 32 (6): 1770-1773. (Zhang Yonghong, Zhang Bo. Image encryption algorithm based on Logistic chaotic system [J]. Application Research of Computers, 2015, 32 (6): 1770-1773)

[11] Mohd B J, Abed S, Al-Hayajneh T, *et al.* FPGA hardware of the LSB steganography method [C]// Proc of International Conference on Computer, Information and Telecommunication Systems. 2012: 1-4.

[12] Farid H, Lyu S. Higher-order wavelet statistics and their application to digital forensics [C]// Proc of Conference on Computer Vision and Pattern Recognition Workshop. 2003: 94-94.